

Regulation and Protection of Social Media Crime for Teenagers

Aparna Singh Chauhan¹, Dr. Sandeep Kumar²

¹ Research Scholar, Department of Legal study, Motherhood University Roorkee (Uttarakhand)

Email: chauhanaparna28@gmail.com

² Assistant Professor, Department of Law, Motherhood University Roorkee (Uttarakhand)

Email: behappysk9@gmail.com

Abstract

Social media has become an important part of a teenager's daily life these days. With the rapid growth of social media, information is readily accessible. Since its advent, it has become the most widely used platform among teenagers, including platforms like YouTube, Instagram, Facebook, and TikTok. Today most teenagers have smartphones and they spend most of their time online. This has created new opportunities for interaction, learning, and entertainment. While the advent of social media has accelerated work and provided people with new information, it also has disadvantages that can prove dangerous for teenagers and the general public. The advent of social media has also increased the risk of social media crimes such as cyberbullying, identity theft, online harassment, privacy violations, misinformation, and online gaming exploitation. Teenagers are particularly vulnerable due to their lack of knowledge about digital security, emotional sensitivity, and frequent online interactions, and they may be reluctant to give up social media. Today, new things have emerged on social media, attracting teenagers, which leads them to use social media platforms even if they don't want to. This research paper examines the nature and impact of social media crimes affecting teenagers and analyzes the laws and regulatory frameworks that have been created to address these challenges. It also highlights the role of governments, institutions, parents, and social media companies in creating a safe environment. The research paper also discusses protection tools and the role of parents age appropriate regulations, cyber safety education, and effective enforcement of cyber laws are also discussed. The research paper aims to educate and educate teenagers about social media, promote safe online interactions and more.

Keywords: *Social media crime, cyber security, teenagers protection, privacy protection digital safety.*

1. Introduction

Social media is defined as a technology-based platform that is a significant part of adolescents' daily lives. In the USA, 90 percent of adolescents use social media platforms. The amount of time adolescents spend on social media has had a significant impact on their mental health. As a result, local and national initiatives have been launched to ban and restrict social media use. Evidence suggests that such restrictions on adolescents have a negative impact on their mental health. We should focus more on promoting emotional regulation in adolescents so that they can control their over-activity on social media. Young people are increasingly using platforms like YouTube, Instagram, Facebook, WhatsApp, Snapchat, and TikTok. Today, people of all ages and backgrounds are using social media through the internet. However, the number of teenagers involved is

high. Teens are using it to connect and socialize with new people. However, this has also created many challenges for young people, including privacy violations, hate speech, and sexual exploitation. This research aims to promote media safety and provide information to both teens and adults. These platforms offer benefits, including access to entertainment, global news, and educational resources. Social media has also given rise to new types of crime, including cyberbullying, identity theft, fraud, hacking, phishing, cyberstalking, and misinformation. These can pose a greater threat to young people who are highly active on these platforms. Many young people are unaware of these risks, and these young people are often more vulnerable to exploitation. Cybercrime is more difficult to detect because it occurs in a virtual space, where the perpetrators cannot be traced, as they commit these crimes via computer.

2. What is Cyber Crime

Cybercrime refers to any criminal act involving a computer, network, or network device. When a criminal commits a crime using a computer, it is extremely difficult to trace them. In this case, a person is sedentary and uses a computer to commit a crime. These types of crimes are often targeted at juveniles. The consequences can be devastating. These crimes can range from harassment, bullying, child pornography, grooming, and even trafficking. According to the Indian Home Ministry, cybercrime against children in India has increased by more than 400 percent in the last five years, with social media platforms being a major factor. When discussing cybercrime in the context of children and social media, it encompasses a wide range of crimes -

- **Cyber bullying** - It is a form of harassment that occurs through the use of electronic or communication devices such as computers, mobile phones, laptops, etc. According to UNICEF, cyberbullying is bullying using digital technology to intimidate or annoy the targeted individual. This can occur on social media, messaging platforms, or gaming platforms.
- **Online gaming** - Online gaming can involve some abusive activities with teens. When someone tries to deceive or coerce a minor into doing something sexual, such as asking them to send photos or videos, it can be considered online gaming.
- **Identify theft** - Impersonation is the deliberate use of another person's identity to gain financial gain to the detriment of another person, which involves misappropriating personal data, such as name, photo details, etc.
- **Sextortion** - This involves the sexual exploitation of adolescents. Children are threatened and blackmailed. The perpetrators demand nude photos from the children, threatening to share them publicly, and even demand money for the photos.
- **Email spoofing** - In this, an email is sent to a person that appears genuine but is not genuine. Such emails are sent to extort money from the person.
- **Being exposed to inappropriate content** - This includes information, images, or material intended for adults. It may also contain inappropriate or unnecessary material that could incite a child to engage in inappropriate behavior. This includes hate speech and pornography. These crimes affect a person's emotions, sometimes leading to suicide.
- **Cyber grooming** - It's rapidly increasing among teens. Perpetrators develop emotional connections with children through social media or messaging, with the aim of gaining their trust and then sexually exploiting them. Perpetrators create fake accounts and pose as children. Many people are exploited online by this type of perpetrator. This perpetrator can even be an acquaintance.

2.1 Understanding Cyber Crime and Social Media

Social media platforms like Facebook, Instagram, WhatsApp, and Snapchat are essential for children and teenagers to communicate. These platforms are also a hotbed for cybercriminals to exploit teenagers to commit crimes. It's important to understand cybercrime and how it connects with social media, leading to crime.

2.2 Features of Social Media that enable Cyber Crime

- Anonymity and fake profiles
- Private messaging and disappearing chats
- User-generated content and algorithms

3. Role of Government in Regulation

The government has now become aware of cybercrime and is also trying to deal with these crimes. For this, the government has made various types of laws. Some laws already exist in India and some laws have been introduced later. If the old laws are not sufficient to stop the crime, then it becomes necessary to bring new laws. Information Technology Act 2000, Protection of Children from Sexual Offences (POCSO) Act 2012, Indian Justice Code (BNS) 2023, Indian Evidence Act 2023, Indian Civil Protection Code (BNSS) 2023.

4. Legal framework protecting teenager(children)

Global and national efforts have been initiated in the cyber space to create a strong legal framework for the safety of children. India has several laws for cyber law. Laws have also been enacted for children. Implementation of laws faces challenges due to changes in technology, cross-border jurisdiction issues and anonymity of online platforms. It analyses both Indian and international laws and highlights their strengths and weaknesses. International bodies such as the United Nations (UN) and the International Telecommunication Union (ITU) have taken significant steps toward the protection of children in the digital age.

4.1. 1 United Nations Convention on the Rights of the Child (UNCRC)

The UNCRC, ratified by India in 1992, lays the groundwork for the protection of children's rights in all spheres, including the digital one. Articles 16 and 17 emphasize a child's right to privacy and access to appropriate information.²² While the Convention predates widespread internet usage, its principles are relevant to online safety. In 2021, the UN Committee on the Rights of the Child adopted General Comment No. 25, which specifically addresses children's rights in the digital environment, urging states to ensure protection against digital risks while promoting access to beneficial online content.

4.1 2 ITU's Child Online Protection (COP) Guidelines

The ITU's COP Guidelines, updated in 2020, are a comprehensive set of recommendations for governments, industry, parents, and educators. They stress the importance of age-appropriate content, platform accountability, and international cooperation.

4.2 Indian Legal Framework

India has developed a multi-layered legal architecture to protect children against online crimes. This includes both general cyber laws and child-specific protections.

4.2 1 The Information Technology Act, 2000 (IT Act)

The IT Act is the primary legislation governing cyber activities in India. Several provisions are applicable to crimes involving minors:

- **Section 66E:** Punishes the violation of privacy by capturing, publishing, or transmitting images of private areas without consent.
- **Section 67 and 67B:** Address the publication or transmission of obscene material and explicitly prohibit child pornography and exploitative content involving minors.

- **Section 69A:** Grants the government authority to block websites or platforms that host harmful or illegal content.

However, these sections often fall short when it comes to swift enforcement, especially when dealing with foreign-based platforms like Facebook or Instagram that operate under different legal jurisdictions.

4.2 2 Protection of Children from Sexual Offences (POCSO) Act, 2012

The POCSO Act criminalizes a wide range of sexual offenses against children and includes provisions for digital evidence and online exploitation:

- **Section 11 and 12:** Define and penalize sexual harassment, including online gestures or messages of a sexual nature.
- **Section 13–15:** Specifically address the use of children in pornography, including online transmission and storage of such content.
- **Section 27:** Ensures the confidentiality of the child victim's identity and protection during trial. POCSO has become crucial in prosecuting cyber grooming and sextortion cases. Still, challenges like lack of digital literacy among law enforcement and procedural delays hinder timely justice.

4.2 3 Bharatiya Nyaya Sanhita(BNS), 2023

It came into effect on July 1, 2024, replaces the Indian Penal Code (IPC). Sections of the BNS are also invoked in cybercrime cases against children, including:

Section 78 (1) Any man who (i) follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or (ii) monitors the use by a woman of the internet, e-mail or any other form of electronic communication, commits the offence of stalking: Provided that such conduct shall not amount to stalking if the man who pursued it proves that—

- (i) it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or
- (ii) it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or
- (iii) in the particular circumstances such conduct was reasonable and justified.

(2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.

Section 79- Whoever, intending to insult the modesty of any woman, utters any words, makes any sound or gesture, or exhibits any object in any form, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to three years, and also with fine.

Section 351-357- Criminal intimidation, which includes threats made via digital platforms. Though not originally designed for cyber-related offenses, these provisions are frequently adapted to fit digital crimes.

4.3 Recent Legislative and Regulatory Developments

India has been making strides toward digital regulation to protect users especially children.

4.3.1 The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

These rules impose stricter accountability on social media intermediaries:

- Require platforms to remove offensive content within 24–72 hours of complaint.
- Mandate the appointment of grievance officers.
- Enforce age verification mechanisms for content hosting services.

While the intent is commendable, implementation has been uneven. Critics argue that tech companies often delay compliance or interpret the rules loosely.

4.4 Data Protection Laws (Proposed Digital Personal Data Protection Act, 2023)

The Digital Personal Data Protection Act, passed in 2023, provides explicit provisions for processing children's data:

- Defines a "child" as an individual under 18 years of age.
- Requires verifiable parental consent for data collection and processing
- Prohibits tracking, behavioral advertising, or targeted messaging to children.

These provisions echo similar laws like the Children's Online Privacy Protection Act (COPPA) in the U.S., but critics fear poor enforcement due to lack of infrastructure and awareness.

4.5 Gaps and Challenges in the Legal Framework

Despite the presence of multiple laws, several gaps persist:

- **Jurisdictional Issues:** Offenders may operate from outside India, making enforcement difficult.
- **Delayed Investigation and Poor Forensics:** Many police stations lack technical capacity to trace digital crimes.
- **Platform Evasion:** Many social media platforms fail to verify users' ages or act quickly on abuse reports.
- **Underreporting:** Victims, especially children, often feel scared or ashamed to report incidents. These gaps necessitate a more integrated and proactive approach involving legal reform, better policing, and public-private collaboration.

5. Role of Parents, Schools, and Civil Society

While laws and platform policies are important, they alone cannot guarantee the online safety of children. The ecosystem of protection must include parents, educators, and civil society, who serve as the first line of defense. Digital literacy, awareness, and community engagement are essential for creating a safe and empowering online experience for children.

6. Role of Parents in Digital Guardianship

Parents play the most crucial role in protecting children online, but many are unaware of the specific risks or lack the digital skills to respond appropriately.

- Strengthen the IT Act and POCSO
- Data Protection Legislation for Children
- Fast Track Cybercrime Units
- Legal Accountability of Platforms

Conclusion

The rapid development of digital technology has also created new challenges. While digital technology has given rise to new possibilities, it also has its drawbacks, and adolescents are the most vulnerable, including cyber grooming, bullying, identity theft, and online sexual exploitation. This research shows that the prevalence of cybercrime among adolescents in India is a matter of concern and requires urgent action. While the Information Technology Act 2000 and the POCSO Act 2012 exist, they lack protection in the cyber space. The Digital Personal Data Protection Act 2023 provides protection, but a stronger law is needed to prevent online crimes committed by adolescents. Therefore, a special regulatory system is needed for children. Despite the existence of policies at social media companies, they are not properly enforced. Parents, schools, and civil society play an equally important role in this endeavor. Institutions and colleges should educate adolescents about cybercrime and how to prevent it.

References

1. Ministry of Electronics and Information Technology. Information Technology Act, 2000.
2. Government of India. Protection of Children from Sexual Offences Act, 2012.
3. Ministry of Electronics and Information Technology. Digital Personal Data Protection Act, 2023.
4. UNICEF India. Child Online Protection in India: Report, 2022. www.unicef.org/india
5. Internet and Mobile Association of India. Digital Adoption and Online Safety Report, 2023.
6. Centre for Internet and Society. Children Online: A Study on Abuse Reporting Mechanisms, 2022.
7. Childline India Foundation. Annual Report on Child Safety, 2022. www.childlineindia.org.in
8. Cyber Peace Foundation. Digital Shakti Campaign Report, 2023. <https://www.cyberpeace.org>
9. Delhi High Court. XYZ v. Meta Platforms Inc., 2023. www.IndianKanoon.com
10. Bombay High Court. Reena Sharma v. Union of India, 2022. www.livelaw.in
11. Government of UK. Online Safety Act, 2023. www.gov.uk
12. Office of the eSafety Commissioner, Australia. Annual Report 2022–2023. www.esafety.gov.au
13. U.S. Federal Trade Commission. Children’s Online Privacy Protection Rule (COPPA). www.ftc.gov
14. Karnika Seth, CYBER LAWS in the Information Technology ,Universal Law Publishing ,1 January 2009.
15. Bharatiya Nyaya Sanhita (BNS)2023, Taxmann Publications Private Limited, 22 November 2024
16. Talat Fatima ,Cyber Crimes, Bharat Law House.